UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,615	07/30/2001	Phillip W. Rogaway	ROG01-0002	3083

22835 7590 01/25/2005

A. RICHARD PARK, REG. NO. 41241
PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95616

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Acti n Summary	Application No.	Applicant(s)	
	09/918,615	ROGAWAY, PHILLIP W.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears n the c ver sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *30 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *1-66* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-41,50-52, and 61 are drawn to a cryptographic method of encrypting and decrypting a message.

II. Claims 42-44,53-55, and 62-63 are drawn to a first variation of generating offsets.

III. Claims 45-46,56-57, and 64 are drawn to a second variation of generating offsets.

IV. Claims 47-49,58-60, and 65-66 are drawn to a third variation of generating offsets.

The inventions are distinct, each from the other because:

Invention I is a cryptographic method which is a combination and may employ subcombination inventions II, III, or IV. Inventions II, III, or IV could be used independently as offset generation mechanisms in another cryptographic method. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, inventions II, III, or IV have separate utility because they can be used in cryptographic methods without invention I. See MPEP 806.05(d).

Inventions II, III, and IV all discuss different offset generation mechanisms. As one can see from the discussion below, inventions II, III, and IV are all unique offset generation mechanisms which are independent of each other and are thus separate inventions.

Inventions II and III are unrelated. Inventions are unrelated if it can be shown that they are not disclosed as capable of use together and they have different modes of operation, different functions, or different effects. (MPEP 806.04, MPEP 808.01). In the instant case, Invention II discloses "defining the ith offset in the sequence of offsets as the xor of the prior offset and a basis offset associated to the number i" while invention III discloses "computing each subsequent

offset by n-bit computer addition of the prior offset and a stride, and further followed by computer addition of the said constant whenever the first addition resulted in a carry". Since inventions II and III disclose different methods for computing the sequence of offsets, the two inventions are unrelated and not capable of being used together.

Inventions II and IV are unrelated. Inventions are unrelated if it can be shown that they are not disclosed as capable of use together and they have different modes of operation, different functions, or different effects. (MPEP 806.04, MPEP 808.01). In the instant case, Invention II discloses "defining the ith offset in the sequence of offsets as the xor of the prior offset and a basis offset associated to the number i" while invention IV discloses "computing a sequence of offsets using the key variant and the nonce". Since inventions II and IV disclose different methods for computing the sequence of offsets, the two inventions are unrelated and not capable of being used together.

Inventions III and IV are unrelated. Inventions are unrelated if it can be shown that they are not disclosed as capable of use together and they have different modes of operation, different functions, or different effects. (MPEP 806.04, MPEP 808.01). In the instant case, Invention III discloses "computing each subsequent offset by n-bit computer addition of the prior offset and a stride, and further followed by computer addition of the said constant whenever the first addition resulted in a carry" while invention IV discloses "computing a sequence of offsets using the key variant and the nonce". Since inventions III and IV disclose different methods for computing the sequence of offsets, the two inventions are unrelated and not capable of being used together.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

The case presents a burden on the examiner because Inventions I, II, III, and IV are classified distinctly and the search for prior art warrants conducting separate searches. Invention I is a cryptographic method, which is classified in 380/37 (*Communication System Using Cryptography, Block/data stream enciphering*). Inventions II, III, and IV are cryptographic offset generation mechanisms, which are classified in 380/59 (*Cryptography, Miscellaneous*).

A complete response to this requirement must include an election of the invention to be examined, even if the requirement is traversed.

Conclusion

A shortened statutory period for response to this action is set to expire one month (not less than 30 days) from the mail date of this letter. Failure to respond within the period for response will result in ABANDONMENT of the application (see 35 U.S.C. 133, M.P.E.P. 710.02, 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER